



Department of Homeland Security IAIP Directorate Daily Open Source Infrastructure Report for 17 February 2005

Current
Nationwide
Threat Level is
ELEVATED
SIGNIFICANT RISK OF
TERRORIST ATTACKS
[For info click here](http://www.dhs.gov/)
<http://www.dhs.gov/>

Daily Highlights

- The Associated Press reports ChoicePoint Inc., which sells consumer data to government agencies and a variety of companies, has acknowledged that several hackers broke into its computer database and may have stolen credit reports, Social Security numbers, and other sensitive information from as many as 35,000 Californians. (See item [6](#))
- The Department of Homeland Security announced that Judge Michael Chertoff has been sworn in as the second Secretary of the Department. (See item [27](#))
- The Associated Press reports a pipe bomb was found and safely dismantled at a California Department of Motor Vehicles office in what authorities are probing as a possible string of eco-terror-related incidents. (See item [40](#))

DHS/IAIP Update *Fast Jump*

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal, State and Local: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS/IAIP Products & Contact Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://esisac.com>]

1. *February 16, Honolulu Advertiser (HI)* — **Wave energy may be in Hawaii's future.** Wave power could be the next big thing in renewable energy, with a test project off Windward Oahu expected to provide electricity as early as next month. National research programs indicate wave energy is technically feasible and on the verge of being economically competitive with other forms of power generation. The Electric Power Research Institute and the U.S.

Department of Energy's National Renewable Energy Laboratory conducted studies off Waimanalo, as well as in the waters off of four other states. Of those sites, the Hawaii location had the best potential, said the agencies' report. In Hawaii, where 95 percent of electricity is produced from fossil fuels, nearly 90 percent from oil alone, a diversity of energy sources has long been a dream, but it has been slow in coming. As of 2002, according to the federal Energy Information Administration, Hawaii had a total electricity production capacity of 2,267 megawatts. Of that, only 173 megawatts, or seven percent, was produced by renewable energy sources such as hydroelectric and wind power. One goal of the wave-power effort is to find ways to make Navy ocean bases independent of fossil fuels for electricity production.

Source: http://the.honoluluadvertiser.com/article/2005/Feb/16/ln/ln0_2p.html

2. *February 16, Associated Press* — **Protesters disrupt oil trading.** Protesters with foghorns and whistles burst into the International Petroleum Exchange (IPE) in London on Wednesday, February 16, disrupting oil trading in the world's second largest energy futures market on the day the Kyoto Protocol on global warming came into force. The invasion into the trading pit by about 35 demonstrators forced the exchange to suspend open outcry trading for more than an hour. Traders continued to make deals throughout the disturbance by using the exchange's electronic trading platform, the IPE said. Greenpeace spokesperson Ben Stewart said the group was trying to make as much noise as possible to prevent trading and highlight shortcomings of the Kyoto agreement.

Source: <http://www.nytimes.com/aponline/business/AP-Britain-IPE-Prot est.html>

3. *February 15, Department of Energy* — **New contracts awarded for continued fill of Strategic Petroleum Reserve.** The U.S. Department of Energy has awarded two new contracts to deliver crude oil to the Strategic Petroleum Reserve (SPR) this spring under the Royalty-In-Kind (RIK) exchange program. Shell Trading Company and Vitol SA Inc. submitted the best offers and were awarded four-month contracts to deliver 78,000 barrels per day to the SPR, beginning in April. As with all recent oil delivery contracts to the SPR, the crude oil will come from exchange arrangements the companies make for RIK crude produced from federal offshore leases in the Gulf of Mexico and owed to the U.S. government. The department awarded contracts to companies offering the highest exchange value of specification-grade oil for the SPR. Approximately 680 million barrels of oil are currently stored in the SPR's underground salt caverns located along the Gulf Coast of Louisiana and Texas. The SPR is estimated to reach 700 million barrels in inventory later this year.

Source: http://www.energy.gov/engine/content.do?PUBLIC_ID=17463&BT_C ODE=PR_PRESSRELEASES&TT_CODE=PRESSRELEASE

4. *February 15, Associated Press* — **Protesters get jail time for power plant entry.** Six Greenpeace activists were sentenced Tuesday, February 15, to jail terms ranging from five to 30 days for climbing a smokestack at a coal-fired power plant in protest of President Bush's energy policy last year. The protesters cut a hole in a fence that surrounds Allegheny Energy's Hatfield Ferry Power Station about 40 miles south of Pittsburgh, PA, on June 23, then climbed the 700-foot smokestack and unfurled a 2,500-square-foot banner. The six pleaded guilty Tuesday in Greene County Court to misdemeanor charges of reckless endangerment, failure to disperse, disorderly conduct and defiant trespass, according to Tom Wetterer, general counsel for Greenpeace.

Source: <http://www.phillyburbs.com/pb-dyn/news/103-02152005-450815.h tml>

[\[Return to top\]](#)

Chemical Industry and Hazardous Materials Sector

Nothing to report.

[\[Return to top\]](#)

Defense Industrial Base Sector

5. *February 16, Seattle Post-Intelligencer (WA)* — **Officials from European Aeronautic Defense and Space talk with officials about tanker plant.** Representatives from 35 states met on Tuesday, February 15, with officials from Boeing Co.'s fiercest rival to learn more about a \$600 million plan for a manufacturing plant that would produce a new generation of aerial tankers for the Air Force. The session, sponsored by European Aeronautic Defense and Space Co. (EADS), the parent of Airbus, was designed to answer questions from states and communities interested in bidding for the project, EADS spokesperson Guy Hicks said. Hicks said the event was intended to help states and communities decide whether to pursue the project. While the meeting was portrayed as a straight-ahead information session, it was surrounded by complicated subtexts. Boeing won a contract in 2003 to lease and sell 767 aircraft to the Air Force as tankers. The contract was withdrawn last year in the face of corruption charges, and concerns in Congress over the cost. With the Air Force moving to reopen competition for the contract, EADS, a French-based company, wants to convince Pentagon officials and Congress that its plane will be American-made. EADS officials say an American plant would satisfy that demand even though it would largely reassemble pieces manufactured elsewhere in the U.S. and around the world.

Source: http://seattlepi.nwsourc.com/business/212207_airbus16.html

[\[Return to top\]](#)

Banking and Finance Sector

6. *February 16, Associated Press* — **Hackers may have stolen Californians' data.** A company that collects consumer data warned thousands of Californians that hackers penetrated the company's computer network and may have stolen credit reports, Social Security numbers and other sensitive information. ChoicePoint Inc., which sells such data to government agencies and a variety of companies, acknowledged Tuesday, February 15, that several hackers broke into its computer database and purloined data from as many as 35,000 Californians. Last fall, hackers apparently used stolen identities to create what appeared to be legitimate businesses seeking ChoicePoint accounts, said Chuck Jones, a spokesperson for Alpharetta, GA-based company. They opened about 50 accounts. The attack appears to have resulted in at least six cases of identity theft in Los Angeles County. It's unclear whether the data of people outside California was exposed, but law enforcement agents, who have arrested one person on six counts of theft, say hundreds of thousands of Americans elsewhere may be at risk. ChoicePoint has not notified consumers in other states, nor is it working with law enforcement agents elsewhere, Jones said.

Source: <http://www.nytimes.com/aponline/technology/AP-ChoicePoint-Hacking.html?>

7. *February 16, Finextra Research* — **Regulators issue outsourcing guidance.** Securities and banking industry regulators have spelled out the risks involved in outsourcing and issued a set of core principles for financial firms to follow when moving business out of house. The publication of the reports — by the cross-industry regulatory Joint Forum and the International Organization of Securities Commissions (IOSCO) — follows an extended consultation process with industry participants. The Joint Forum principles focus on establishing coherent policy and risk management programs for outsourcing activities. Issues for consideration in drawing up contracts and contingency planning are also discussed. The IOSCO report follows a survey of industry participants which found that a clear majority of firms in all jurisdictions has in place some form of outsourcing arrangement. The chairman of the IOSCO Technical Committee, Andrew Sheng, says, "The results of our survey on outsourcing indicate that financial intermediaries are outsourcing significant aspects of their business activities to service providers." Joint Forum Report: <http://www.iosco.org/pubdocs/pdf/IOSCOPD184.pdf> IOSCO Report: <http://www.iosco.org/pubdocs/pdf/IOSCOPD187.pdf> Source: <http://www.finextra.com/fullstory.asp?id=13253>

8. *February 16, Vnunet.com* — **Online fraud hits record levels.** Nearly 10 million people suffered from some kind of online fraud last year, according to figures released on Wednesday, February 16, by Gartner at the RSA Conference in San Francisco, CA. The analyst firm's survey of U.S. consumers estimated that fraudsters had hit 9.5 million people last year. The total amount was \$1.2 billion, the bulk of which was stolen by criminal gangs in Eastern Europe and African states. Avivah Litan, research director of payments and fraud at Gartner, explained that, while levels of traditional fraud like stolen checks had remained relatively constant, information theft was rising sharply. This was reflected in higher levels of fraudulent transfers of money from bank accounts. These levels of fraud would drive investments in security technology, Litan added, which would include better authentication of users and a move away from passwords. By 2007, she predicted that 75 percent of U.S., and 70 per cent of worldwide, banks would no longer rely on passwords alone to protect online accounts. Source: <http://www.vnunet.com/news/1161282>

9. *February 15, Department of the Treasury* — **Treasury takes action to stem funding to the Iraqi insurgency.** The U.S. Department of the Treasury again took action on Tuesday, February 15, against an individual whose efforts were helping to finance the Iraqi insurgency, as well as al Qaeda. "Today's designation of al-Fadhli is another important step in breaking the financial ties the al-Zarqawi Network depends on to perpetrate acts of horror and violence against people of all faiths and nationalities," said Treasury Secretary John W. Snow. Muhsin al-Fadhli was designated under Executive Order 13224 for providing financial and material support to the al-Zarqawi Network and al Qaeda. The U.S. is submitting al-Fadhli to the United Nations 1267 Committee, which will consider adding him to the consolidated list of terrorists tied to al Qaeda, Osama bin Laden and the Taliban. Muhsin al-Fadhli is considered an al Qaeda leader in the Gulf countries. Information available to the U.S. Government indicates that al-Fadhli fought alongside the Taliban and al Qaeda in Afghanistan. Muhsin al-Fadhli's support for terrorism extends to Iraq where he is believed to be providing support to fighters against U.S. and multinational forces and is considered a major facilitator connected to the brutal terrorist, Abu Musab al-Zarqawi. Source: <http://www.treasury.gov/press/releases/js2252.htm>

10. *February 14, Silicon.com* — **UK businesses targeted by identity hijack scam.** UK firms are being warned about a new online scam that targets the Companies House database in an attempt to hijack the identity of registered companies. Companies House is a UK government entity that incorporates and dissolves limited companies. The scam involves fraudsters accessing a form on the Companies House Website to change the registered office for a limited company. The only details they need to do this are the head office postal address and registered company number, which can easily be searched for on the Internet. Companies House does not notify firms of any change in address. The fraudsters then change the address to a mailbox address or rented residential property, which they can use to open trade accounts and to which they can have goods delivered. Online fraud prevention firm Early Warning discovered the scam and said firms whose details have been hijacked will only find out when the debt collectors arrive or legal action is initiated to recover goods that have been fraudulently obtained. A Companies House spokesperson said that they encourage firms to file all documents electronically using their new online filing system, which requires a unique security code for changes to be made. Source: <http://software.silicon.com/security/0,39024655,39127843,00.htm>

[\[Return to top\]](#)

Transportation Sector

11. *February 16, Washington Post* — **Legislators oppose raising airline ticket security fees.** Senate Republicans and Democrats united in criticism on Tuesday, February 15, against the Bush Administration's proposal to increase security fees on airline tickets, saying that the costs of securing the nation's aviation system should be paid for by the government. The administration has proposed adding \$3 to the existing \$2.50 fee airline passengers pay for each flight. Fees would be capped at \$8 for one-way tickets that involve multiple stops, and at \$16 for a round-trip ticket. Lawmakers said they opposed the proposed fee increase because it would not provide additional funds to improve airline security. Instead, the estimated \$1.5 billion raised by the new fee would simply replace funds now provided by the government. No senators voiced support, and some representing rural areas argued that their constituents would be hit disproportionately hard because nonstop air service is not available from many of the communities. Passengers who need to connect through a hub airport to reach their destination would incur twice the fees as those who fly nonstop because the fee is levied for each flight segment. Source: <http://www.washingtonpost.com/wp-dyn/articles/A27259-2005Feb 15.html?sub=AR>

12. *February 16, Associated Press* — **Northwest will stop free food service, adds choices to buy.** Northwest Airlines plans to eliminate free meals on all its domestic flights for coach passengers, starting March 1. The Eagan, MN-based airline instead will offer travelers a choice of buying a \$3 snack box or a \$5 sandwich. The move is expected to save Northwest between \$20 million and \$30 million annually. Northwest is following other airlines, such as U.S. Airways and American Airlines, that have eliminated complimentary meals in coach service. Elimination of the complimentary meal service will start with about 450 daily flights and expand by July 1 to 900 flights — about 60% of the airline's flights. Northwest has about 1,500 daily flights. Meals served to business and first-class passengers on Northwest, as well as all passengers flying to Europe and Asia, will not be affected.

Source: http://www.usatoday.com/travel/news/2005-02-16-new-food_x.htm?POE=TRVISVA

13. *February 16, Associated Press* — **Judge cuts United's debt obligation to O'Hare.** A bankruptcy judge approved a deal Tuesday, February 15, dramatically reducing how much of O'Hare International Airport's debt United Airlines must pay. The deal, reached earlier with bondholders, will save United about \$450 million and help the nation's number two carrier emerge from bankruptcy, United spokesperson Jeff Green said. It slashes United's obligation to pay \$600 million of O'Hare's debt by 75 percent. The debt is from bonds the Chicago airport sold to United to fund construction projects specifically for the airline, Green said. United, a unit of Elk Grove Village, IL-based UAL, hopes to reach similar agreements with airports in New York, Denver, San Francisco and Los Angeles, he said.

Source: http://www.usatoday.com/travel/news/2005-02-16-united-ohare_x.htm

14. *February 16, Department of Transportation* — **Transportation Secretary Mineta announces grants for Louisiana.** Federal grants totaling approximately \$33.7 million will help to expand capacity and enhance safety at airports throughout Louisiana, U.S. Transportation Secretary Norman Y. Mineta announced Wednesday, February 16. Twenty-one airports will receive money for projects that include rehabilitating and extending runways, constructing taxiways, and improving runway safety areas. The funds come from the Airport Improvement Program of the U.S. Department of Transportation, s Federal Aviation Administration. "Increasing air traffic is helping to sustain economic expansion in Louisiana and throughout the United States," Secretary Mineta said. "These grants will help Louisiana's airports maintain the highest standards of safety and expand their capacity as air traffic continues to grow."

Source: <http://www.dot.gov/affairs/dot2905.htm>

15. *February 16, TechNewsWorld* — **Boeing aircraft introduces new passenger aircraft.**

Nonstop flights between Britain and Australia were made possible Tuesday, February 15, with the launch of the world's newest passenger aircraft. The 777-200LR will carry 301 passengers 9,420 miles — far enough to fly from Edinburgh, Scotland, to Perth, Australia. The 777-200LR is the fifth variation of Boeing's twin-aisle 777 plane. Better fuel efficiency from engines and lighter materials mean it can connect almost any two cities worldwide. It can fly from London to Sydney non-stop — but cannot make the return journey in one go because of prevailing headwinds. The twin-engine aircraft has been designed by the U.S. manufacturer as a rival to the four-engine Airbus A340-500, which has been in service for more than a year. Boeing expects to sell about 500 of the planes over the next 20 years. It already has orders from Pakistan International Airlines — which will use it to launch 19-hour flights between Karachi and Houston, TX, — and EVA Air, of Taiwan.

Source: <http://www.technewsworld.com/story/news/40650.html>

16. *February 15, Associated Press* — **Airport officials consider new superjumbo hassles.** U.S. airports from Seattle to Atlanta say accommodating Airbus SAS's new superjumbo A380 in anything other than an emergency would require major construction. Runways would need widening and terminals would need upgrades to load and unload the double-decker plane easily. Even with those improvements, airports might need to curtail other airport traffic to let the big jet lumber through the airfield. Some officials worry the weight of the A380 would collapse tunnels and buckle overpasses. Stretching about three-quarters of the length of a

football field, the A380 isn't much longer than Boeing Co.'s latest version of the 747, currently the largest commercial airplane in the skies. But the A380's 261-foot wingspan is 50 feet wider than the 747, broader than many runways and taxiways were built to accommodate. The airplane also weighs in at a maximum of 1.2 million pounds, 30 percent more than the biggest 747. The Federal Aviation Administration (FAA) says just four U.S. airports — John F. Kennedy in New York, San Francisco, Los Angeles and Miami — are formally working with regulators on plans to accept the new plane for passengers. Another two — Anchorage and Memphis — are working with the FAA to take the cargo version.

Source: <http://www.cnn.com/2005/TRAVEL/02/15/bt.airbus.airports.ap/index.html>

[\[Return to top\]](#)

Postal and Shipping Sector

17. *February 16, Shreveport Times (LA)* — New postal, Internet scams surfacing. Some of the scams are updates of old "work-at-home" schemes, said Marcia Colliver, one of two postal inspectors working out of Shreveport, Louisiana's main postal facility. But others are recent and sophisticated schemes that are high-tech and international in scope, she said. "We're targeting home scams and counterfeit money orders that are disguised as work-at-home offers or sell on the Internet ventures," Colliver said. "Or they're going through 'chat rooms,' asking their victims to contact them on the Internet." Many of the recent attempts have been done using counterfeit postal money orders, many of which seem to originate in Nigeria, she said. "In the last four months, we've handled \$100,000 in counterfeit money orders." Even the old "make money mailing from home" often is a scam, Colliver warned. Scammers — usually overseas but sometimes from another part of the country — will mail packages of pre-sealed envelopes to people to re-mail. "The envelopes contain money orders or checks but have a U.S. postmark, so they look like it comes from inside the U.S. — but it's not," Colliver said. The money orders sometimes are in groups.

Source: <http://www.shreveporttimes.com/apps/pbcs.dll/article?AID=/20050216/NEWS01/502160325/1002/NEWS>

18. *February 15, Government Executive* — Postal Service boosts internal controls. When the U.S. Postal Service (USPS) decided to add functions to employees' Blackberrys, it turned to Peg Weir to make sure it was properly securing the wireless devices. When the gadgets are rolled out next month, they will have internal controls in place, including password requirements and automatic timing out. As manager of the USPS Internal Control Group, Weir works on developing efficient and secure agency-wide processes. While most agencies have strengthened their internal controls, since the 2002 Sarbanes-Oxley Act, none has gone as far as the USPS. The Internal Control Group, which was created as part of the 2002 Transformation Plan, is responsible for the Postal Service's voluntary compliance to Sarbanes-Oxley, which requires documenting and testing internal controls. Sarbanes-Oxley applies to the private sector, but the Office of Management and Budget recently instructed agencies to strengthen their internal controls in line with that regulation. Weir's group has already made improvements: At their peak, paper and electronic systems that track the eFleet card, a credit card that links to a Web-based tracking system, were off by almost \$11.7 million out of a total of \$63 million in expenditures. Weir's group helped bring that number down to \$1.3 million.

Source: <http://www.govexec.com/dailyfed/0205/021505k1.htm>

[\[Return to top\]](#)

Agriculture Sector

19. *February 16, Southeast Farm Press* — **Alabama officials initiate animal identification system.** Alabama agriculture officials have recently initiated the Alabama Premises Registration System, a program designed to identify the origin and location of diseased animals within 48 hours by using a database to track farm animals from birth to market. Perry Mobley, director of the Alabama Farmers Federation Beef Division, says the Alabama Premises Registration System is still in its early stages. "The department goal for 2005 is to have 75 percent of Alabama premises registered. Currently fewer than 1,000 of the more than 45,000 premises in the state are registered." Mobley says the program's biggest challenge will be convincing all farmers to register, including those with few livestock. In addition to registering premises as part of a national animal identification program, the state also boasts the gold standard for individual animal tracking systems -- the Alabama Beef Connection. Consisting of partners from Auburn University and other livestock organizations within the state, the Alabama Beef Connection was originally designed to boost the value of Alabama beef calves, says Lisa Kriese-Anderson, associate professor of animal science at Auburn University. "The Alabama Beef Connection uses carcass data to gauge performance from calves tracked through the marketing chain by an electronic ear tag."

Source: <http://southeastfarmpress.com/news/021605-Alabama-cattlemen/>

20. *February 15, St. Louis Today (MO)* — **Monsanto ups security after threat.** Monsanto Corp. has increased security on its Creve Coeur, MO, campus in response to a non-specific threat made by a caller to a radio talk show. Monsanto security also alerted the Donald Danforth Plant Science Center in Creve Coeur and Solutia Inc. in Town and Country, MO, to the threats made on the Schnitt Show, a syndicated program based in Tampa, FL, and hosted by Todd Schnitt. Content from the program is rebroadcast in St. Louis, MO. An adult male caller to the February 8 Schnitt show identified himself only as Mel and said he was calling from Waco, TX. The caller mentioned Monsanto on and off the air. The caller said he was planning a terrorist attack in the next several weeks that would target "corporate offices, genetic research laboratories, a couple of distribution centers, that sort of thing." Pete Krusing, an FBI spokesperson, said the investigation is centered in Florida.

Source: <http://www.stltoday.com/stltoday/business/stories.nsf/story/4EED5EE4461BEC7386256FA900129F80?OpenDocument&Headline=Monsanto+ups+security+after+threat&highlight=2%2Cmonsanto>

[\[Return to top\]](#)

Food Sector

21. *February 16, Food Production Daily* — **UK agency targets poultry sector to cut foodborne illness.** Food is the most common source of zoonotic infections in humans, suggesting that tightening biosecurity measures at the beginning of the food supply chain is vital. As a result,

the United Kingdom's Food Standards Agency (FSA) is targeting poultry producers to help achieve a 20 percent reduction in the incidence of foodborne diseases by April 2006. The FSA aims to work closely with the farming industry to achieve a 50 percent reduction in the incidence of chickens, which test positive for campylobacter at slaughter by 2010. More than a million tons of chicken meat is produced in the United Kingdom every year, 96 percent of which is from intensive production systems. The first three years of the FSA's campylobacter strategy will focus aggressively on a campaign to improve biosecurity on intensive chicken farms. The idea is that by ensuring that all farms achieve an appropriate standard of biosecurity, the number of campylobacter positive flocks will be reduced.

Source: <http://www.foodproductiondaily.com/news/news-NG.asp?n=58098-fsa-targets-poultry>

[\[Return to top\]](#)

Water Sector

22. *February 16, Arizona Republic* — Officials say water scare could have been averted.

Phoenix, AZ, officials admitted Tuesday, February 15, that January's water contamination scare could have been avoided and that the incident exposed serious vulnerabilities within the city's emergency response network. The advisory was issued at 2:30 a.m. on January 25 without consultation with the City Manager's Office or the Maricopa County health department when it became obvious that the city wouldn't be able to clean the water leaving the Val Vista Water Treatment Plant well enough to meet federal drinking water standards because of high sediment levels. City auditors interviewed 66 people and spent 600 hours looking into why the city failed to treat the water and how it notified the public of the problem. The city's emergency management coordinator was not told of the boil-water advisory and didn't know about it until he turned on the morning news. Key water department personnel did not have appropriate emergency contact numbers, and therefore couldn't get information to the people they needed to. There is no indication that the Water Services Department has ever conducted emergency preparedness or incident training as required by its operating procedures.

Source: http://www.azcentral.com/arizonarepublic/local/articles/0216_water16.html

[\[Return to top\]](#)

Public Health Sector

23. *February 15, Sandia National Laboratories* — Tests confirm the Explosive Destruction System's ability to destroy biological agents.

Researchers at the National Nuclear Security Administration's Sandia National Laboratories, the creators of the Army's Explosive Destruction System (EDS), suspected the system could, in addition to snuffing out chemical warfare material, treat and destroy biohazards. A study at Sandia confirms EDS's effectiveness against biological agents, bio-contaminated containers, and improvised biological devices. The EDS is a proven, transportable system that has safely neutralized and discarded recovered chemical warfare material. The bioagent treatment system for the EDS platform was developed by Sandia, which performed tests with anthrax simulants such as *Bacillus thuringiensis* and *Bacillus stearothermophilus*. The test system was operated in steam autoclave, gas fumigation,

and liquid decontamination modes of operation. Additional tests with chlorine dioxide and chlorine bleach solution were also performed, and the breaking of a glass container was demonstrated to expose the bacterial spores prior to treatment. Each of the three treatment processes used during testing resulted in complete neutralization of the bacterial spores based on no bacterial growth in post-treatment incubations.

Source: <http://www.sandia.gov/news-center/news-releases/2005/def-non-prolif-sec/bio-EDS.html>

24. *February 15, Voice of America* — **Experts say malaria can be eradicated.** Experts on malaria say the obstacle to reducing the disease in Africa is no longer technical, but financial. They point to recent scientific advances against the virus, which they say can dramatically cut its incidence if more money is forthcoming. Leaders of groups fighting malaria briefed congressional staff members on the progress being made in medicines, a vaccine, and other anti-malaria technology. The head of the Global Fund to Fight AIDS, Tuberculosis, and Malaria, Richard Feachem, told the legislative aides the disease continues to spread in Africa needlessly. Feachem says new and well-established technologies are having an impact against malaria wherever they have been combined. They include a recently developed mosquito net from Japan impregnated with long lasting insecticide, indoor insecticide spraying, novel rapid diagnostic techniques, a new combination therapy using the Chinese herb Artemisinin that is more expensive than older treatments but more effective, and automatic treatment of pregnant women. Another promising new technology is an experimental vaccine. Tests last year showed it prevented malaria in 30 percent of the Mozambican children inoculated and kept it from becoming life threatening in nearly 60 percent. The percentages are lower than with vaccines for other diseases, but higher than using bed nets and insecticides.

Source: <http://www.voanews.com/english/2005-02-15-voa67.cfm>

25. *February 14, Center for Digital Government* — **Status of state and local disease surveillance systems.** The Center for Digital Government recently examined from a technology perspective how well a state or local jurisdiction and its affiliated health organizations would be able to respond to a disease outbreak. The Center surveyed 46 states and several large localities to determine to what degree they are effectively utilizing IT in public health preparedness efforts. The study found that 57 percent of the jurisdictions surveyed either had a disease tracking and surveillance system in place or had begun implementing one. According to the Center's survey, only 48 percent of jurisdictions currently implementing a disease tracking and surveillance system are implementing the U.S. Centers for Disease Control and Prevention's (CDC) system. The remaining states are implementing proprietary systems or pursuing other standalone system architectures that employ the CDC standards. Only 35 percent of those jurisdictions expect their systems to be able to collaborate with other state/jurisdictions.

Source: http://media.centerdigitalgov.com/reg2view/CDG04White_Paper_NEDSS_-_Final.pdf

26. *February 01, Emerging Infectious Diseases* — **Animal mortality monitoring and human Ebola outbreaks.** All human Ebola virus outbreaks during 2001–2003 in the forest zone between Gabon and Republic of Congo resulted from handling infected wild animal carcasses. After the first outbreak, Researchers created an Animal Mortality Monitoring Network in collaboration with the Gabonese and Congolese Ministries of Forestry and Environment and wildlife organizations (Wildlife Conservation Society and Programme de Conservation et

Utilisation Rationnelle des Ecosystèmes Forestiers en Afrique Centrale) to predict and possibly prevent human Ebola outbreaks. Since August 2001, 98 wild animal carcasses have been recovered by the network, including 65 great apes. Analysis of 21 carcasses found that 10 gorillas, three chimpanzees, and one duiker tested positive for Ebola virus. Wild animal outbreaks began before each of the five human Ebola outbreaks. Twice researchers alerted the health authorities to an imminent risk for human outbreaks, weeks before they occurred.

Source: <http://www.cdc.gov/ncidod/eid/vol11no02/04-0533.htm>

[\[Return to top\]](#)

Government Sector

27. *February 16, Department of Homeland Security* — Michael Chertoff becomes Homeland Security Secretary. On February 15, 2005, Judge Michael Chertoff was sworn in as the second Secretary of the Department of Homeland Security. Chertoff formerly served as United States Circuit Judge for the Third Circuit Court of Appeals. Secretary Chertoff was previously confirmed by the Senate to serve in the Bush Administration as Assistant Attorney General for the Criminal Division at the Department of Justice. As Assistant Attorney General, he helped trace the September 11 terrorist attacks to the al Qaeda network, and worked to increase information sharing within the FBI and with state and local officials. Prior to that, Chertoff spent more than a decade as a federal prosecutor, including service as U.S. Attorney for the District of New Jersey, First Assistant U.S. Attorney for the District of New Jersey, and Assistant U.S. Attorney for the Southern District of New York. As United States Attorney, Chertoff investigated and prosecuted several significant cases of political corruption, organized crime, and corporate fraud. Chertoff graduated magna cum laude from Harvard College in 1975 and magna cum laude from Harvard Law School in 1978. From 1979–1980 he served as a clerk to Supreme Court Justice William Brennan, Jr.

Source: http://www.dhs.gov/dhspublic/interapp/biography/biography_01_16.xml

[\[Return to top\]](#)

Emergency Services Sector

28. *February 16, Government Technology* — Digital tests to enhance the Emergency Alert System. The Department of Homeland Security's (DHS) Federal Emergency Management Agency (FEMA), the federal government's program manager for the national Emergency Alert System (EAS), along with the Association of Public Television Stations (APTS) and the Department's Information Analysis and Infrastructure Protection (IAIP) Directorate, have joined other federal departments and agencies and several private communication companies and broadcasters for a series of tests using digital technology to improve America's alert and warning system. The tests are part of a one-year pilot project to demonstrate how DHS can improve public alert and warning during times of national crisis through the use of local public television's digital television broadcasts. Called the Digital Emergency Alert System (DEAS) National Capital Region Pilot under DHS' Integrated Public Alert and Warning (IPAWS) initiative, the tests are successfully demonstrating how DHS and the National Oceanic and Atmospheric Administration (NOAA) can disseminate alert and warning messages leveraging

public–private partnership.

Source: <http://www.govtech.net/news/news.php?id=93084>

29. *February 16, Benton County Daily Record (AK)* — Disaster–impact team begins plans.

Although citizens did not attend the first public Benton County Hazard Mitigation meeting on Tuesday, February 15, planners are well on their way to helping reduce the impact of natural disasters. The County Hazard Mitigation planners come from city and county administrations, fire departments, emergency services, hospitals, schools and businesses throughout the county that all have a stake in reducing or eliminating risks from natural hazards. The Federal Emergency Management Agency (FEMA) is urging counties to develop a plan to serve as a guiding document to reduce the impact of natural hazards on the county. The project should be complete by July 1. Once the plan is complete, it will be forwarded to the Arkansas Department of Emergency Management (ADEM) for review. Once the ADEM has reviewed the plan, it will be forwarded to FEMA, Dixon said. Once FEMA has approved the plan, it will be presented to county and city governments for adoption. The objective of the plan is to reduce vulnerability to disasters and increase resistance in Benton County and participating jurisdictions. FEMA believes the plan will reduce the cost of disaster recovery. Since 1993, FEMA spent more than \$20 billion on federal disaster recovery.

Source: <http://nwanews.com/story.php?paper=bcdr§ion=News&storyid=17412>

[\[Return to top\]](#)

Information Technology and Telecommunications Sector

30. *February 16, EE Times* — Chinese researchers claim to have compromised SHA–1 hashing algorithm.

A team of three Chinese researchers claim to have compromised the SHA–1 hashing algorithm at the core of many of today's mainstream security products. Top cryptographers said users can still rely on today's SHA–1–based systems and applications, but next–generation products will need to move to new algorithms. In a panel discussion at the RSA Conference on Tuesday, February 15, Adi Shamir, a celebrated cryptographer and professor at Israel's Weizmann Institute of Science, said he received an e–mail that morning containing a draft technical paper from the research team of Xiaoyun Wang, Lisa Yiqun Yin, and Hongbo Yu who have links to Shandong University in China. The paper described how two separate documents could be manipulated to deliver the same SHA–1 hash with a computation of lower complexity level than previously believed possible. Shamir and others said they believe the work of the Chinese trio will probably be proven to be correct based on their academic reputations, although details of the paper are still under review. Perhaps anticipating the news, the National Institute of Standards and Technology issued a recommendation earlier this month that developers move to SHA–256 and SHA–512 algorithms by 2010.

Source: http://www.eetimes.com/article/showArticle.jhtml?articleId=6_0401254

31. *February 16, Secunia* — HP Web–Enabled Management Software HTTP Server buffer overflow.

A vulnerability has been reported in HP HTTP Server, which can be exploited by malicious people to compromise a vulnerable system. The vulnerability is caused due to an unspecified boundary error within the handling of input parameters and can be exploited to cause a buffer overflow. Successful exploitation may allow execution of arbitrary code. Update to HP HTTP Server 5.96 or Systems Management Homepage version 2.0. Management Software

Security Patch for Windows Version 5.96:

http://h18023.www1.hp.com/support/files/Server/us/download/2_2192.html

Source: <http://secunia.com/advisories/14311/>

32. *February 15, Government Computer News* — **CIOs say consolidation and cybersecurity top priority list.** CIOs and IT managers will focus on systems consolidation and security through the end of the fiscal year. That's the chief finding from a new survey of CIOs from civilian, Defense Department, legislative and top-level executive offices. The driving factors behind IT consolidation are cutting costs and improving network cybersecurity, respondents said in the 15th annual Federal CIO Survey. CIOs also identified risk management, integrating physical and IT security, and assessing the vulnerabilities of less crucial systems as among their top priorities. The survey, conducted by the IT Association of America, found that CIOs want to reduce the number of e-mail, file and print servers in use as well as cut the number of data centers. Survey: http://www.ita.org/news/docs/itaasurvey_f.pdf
Source: http://www.gcn.com/vol1_no1/daily-updates/35066-1.html
33. *February 15, SecurityTracker* — **Sami HTTP Server input validation vulnerabilities.** A remote user can view files on the target system or cause the web service to crash by sending a specially crafted HTTP request containing '..' directory traversal characters to obtain files on the system that are located outside of the web document directory. Encoded directory traversal characters can also be used. The user can also send an HTTP request to cause the web service to crash. There is no solution at this time.
Source: <http://www.securitytracker.com/alerts/2005/Feb/1013191.html>
34. *February 15, SecurityTracker* — **Linux Kernel '/proc' signed integer errors let local users execute arbitrary code.** A vulnerability was reported in the Linux kernel in '/proc'. A local user can execute arbitrary code or view kernel memory to gain elevated privileges. A local user can trigger a buffer overflow or view kernel memory. Some flaws reside in the `proc_file_read()` function in 'fs/proc/generic.c', where a call to `min_t()` uses an incorrect integer definition, and in the `locks_read_proc()` function where an integer parameter is incorrectly defined. A local user can trigger a buffer overflow. The vendor has released a fixed version (2.6.11-rc4), available at: <http://www.kernel.org/>
Source: <http://www.securitytracker.com/alerts/2005/Feb/1013188.html>
35. *February 15, SecurityTracker* — **Sun Solaris can be crashed by a remote user sending a flood of ARP packets.** A vulnerability was reported in Sun Solaris in the processing of ARP packets. A remote user can cause denial of service conditions. A remote user on a local network can send a large number of specific ARP packets to cause the target system to hang. Updates and original advisory at: <http://classic.sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F57673>
Source: <http://securitytracker.com/alerts/2005/Feb/1013179.html>
36. *February 15, Secunia* — **BrightStor ARCserve Backup Discovery Service SERVICEPC buffer overflow.** A vulnerability has been reported in BrightStor ARCserve/Enterprise Backup, which can be exploited by malicious people to compromise a vulnerable system. The vulnerability is caused due to a boundary error in the Discovery Service when processing received network traffic. Successful exploitation allows execution of arbitrary code. Updates

Internet Alert Dashboard

DHS/US-CERT Watch Synopsis	
Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.	
US-CERT Operations Center Synopsis: On Tuesday, Microsoft published 13 security updates as part of their February security release. Eleven of the security bulletins affect Windows, and nine of the bulletins have been marked as "Critical." The US-CERT recommends ensuring that all Windows systems on your network have been patched for these vulnerabilities. Full information on the vulnerabilities, as well as links to the patches can be found at http://www.microsoft.com/security/default.msp	
Current Port Attacks	
Top 10 Target Ports	445 (microsoft-ds), 135 (epmap), 139 (netbios-ssn), 1025 (---), 53 (domain), 1026 (---), 4662 (eDonkey2000), 80 (www), 6346 (gnutella-svc), 1027 (icq)
Source: http://isc.incidents.org/top10.html ; Internet Storm Center	
To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Website: www.us-cert.gov .	
Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it-isac.org/ .	

[\[Return to top\]](#)

Commercial Facilities/Real Estate, Monument & Icons Sector

37. February 15, The Citizen (NY) — New York mall security ready. In light of a shooting at Hudson Valley Mall in Kingston that left two injured, Auburn, NY, officials are confident the Fingerlakes Mall would be prepared if a similar situation were to occur. Gina Speno, Fingerlakes Mall general manager, said attention to security at the mall was heightened after the September 11 attacks, and a security plan is in place that can apply to a variety of situations. "The safety of our shoppers, tenants, and employees is our first priority," she said. "Since 9/11, everyone looks at security a different way." Last Sunday afternoon, Robert Bonelli, 25, entered Best Buy at Hudson Valley Mall in Kingston, NY, and began to open fire. After firing his way through the store, he made his way into the mall corridor and continued shooting. Two shoppers were wounded, one of whom remained in critical condition Monday. Concern for security at the mall increases with the addition of tenants, which bring more shoppers, said Cayuga County Sheriff Rob Outhouse. But he's pleased with how the mall's security has adapted to meet the challenges. "There's an obvious change in the way security is handled there," he said. "It's a more hands-on security force."

Source: <http://www.auburnpub.com/articles/2005/02/15/news/news03.txt>

General Sector

38. *February 16, Los Angeles Times* — U.S. recalls ambassador to Syria. The U.S. ambassador to Syria was called back to Washington on Tuesday, February 15, as anger swelled against Damascus after the assassination of former Lebanese Prime Minister Rafik Hariri. In Beirut, Lebanon, where Hariri was killed by a car bomb Monday, February 14. Mobs attacked Syrian laborers in southern Lebanon and burned tires outside a Syrian government building in Beirut. The Lebanese army went on alert, and flatbed trucks loaded with soldiers appeared on street corners throughout Beirut. It is unclear who engineered the attack that killed Hariri and at least nine others. Hariri quit as prime minister in October in protest of Syria's tampering in Lebanese affairs. Damascus has for months ignored a United Nations Security Council mandate to withdraw its forces from neighboring Lebanon. Even before the U.S.-led invasion of Iraq in March 2003, Washington had accused Syria of harboring terrorists, pursuing biological and chemical weapons and failing to cooperate in the U.S.-declared war on terrorism. After the fall of Saddam Hussein, the U.S. accused Syria of allowing foreign fighters to stream across its border into Iraq, of giving shelter to people who were directing the Iraqi insurgency, and of allowing elements of the Iranian regime to operate from Syrian territory.

Source: <http://www.latimes.com/news/nationworld/world/la-fg-syria16feb16.0.2210147.story?coll=la-home-headlines>

39. *February 16, Boston Globe* — Teacher allegedly gave bomb-making lesson. A Florida high school chemistry teacher was arrested after students claimed he taught his class how to make a bomb, authorities said. David Pieski, 42, used an overhead projector in class to give instructions in making explosives to students at Freedom High School in Orlando, FL, including advising them to use an electric detonator to stay clear from the blast, an Orange County sheriff's arrest report said. In Pieski's classroom, authorities found a book labeled "Demo," which includes the chemical breakdown for a powerful explosive, the arrest report said. One student said he set off an explosive device at a golf course on January 6 and videotaped it, an arrest warrant said. Pieski was charged with possessing or discharging a destructive device and culpable negligence. Pieski, who was booked into the Orange County Jail on Monday and released on \$1,000 bail, declined to comment. School officials told investigators that Pieski previously had been told he was not allowed to have any form of explosive on campus.

Source: http://www.boston.com/news/nation/articles/2005/02/16/teacher_allegedly_gave_bomb_making_lesson/

40. *February 15, Associated Press* — Eco-terror probed in fifth bomb finding. A pipe bomb was found and safely dismantled at the Department of Motor Vehicles office in Auburn, CA, on Tuesday, February 15. It was the latest in what authorities are probing as a possible string of eco-terror-related incidents in communities east of Sacramento. A different type of homemade explosive device was found Sunday, February 13, outside the Placer County Courthouse in Auburn and also dismantled by the county sheriff's bomb squad robot. The FBI's Joint Terrorism Task Force is investigating a series of recent incidents, two of which have been claimed as the work of the Earth Liberation Front, a shadowy environmental extremist group. "We're certainly not discounting that they all could be related, but we haven't made that leap,"

said FBI spokesperson Karen Ernst. "No one has claimed responsibility for these (latest two) incidents," she said. The latest device was discovered about 7 a.m. Tuesday at the back of the state motor vehicles department office, Ernst said. While the first three fire bombings were aimed at developments, the last two have targeted government establishments, she noted.

Source: http://www.mercurynews.com/mld/mercurynews/news/local/states/california/northern_california/10908051.htm?1c

[\[Return to top\]](#)

DHS/IAIP Products & Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures:

[DHS/IAIP Daily Open Source Infrastructure Reports](#) – The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open–source published information concerning significant critical infrastructure issues. The DHS/IAIP Daily Open Source Infrastructure Report is available on the Department of Homeland Security Website: <http://www.dhs.gov/iaipdailyreport>

[Homeland Security Advisories and Information Bulletins](#) – DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact. Homeland Security Advisories and Information Bulletins are available on the Department of Homeland Security Website: <http://www.dhs.gov/dhspublic/display?theme=70>

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883–3644.

Subscription and Distribution Information:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883–3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282–9201.

To report cyber infrastructure incidents or to request information, please contact US–CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is a non–commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.